



ELECTRONIC MAIL SYSTEM, METHOD FOR PREVENTING TRANSMISSION OF IMPERSONATED ELECTRONIC MAIL, AND METHOD FOR PREVENTING RECEPTION OF IMPERSONATED MAIL

Publication number: JP2004064215
Publication date: 2004-02-26
Inventor: NARUSE KENICHI
Applicant: CASIO COMPUTER CO LTD
Classification:
 - International: H04L12/58; H04L12/58; (IPC1-7): H04L12/58
 - European:
Application number: JP20020216759 20020725
Priority number(s): JP20020216759 20020725

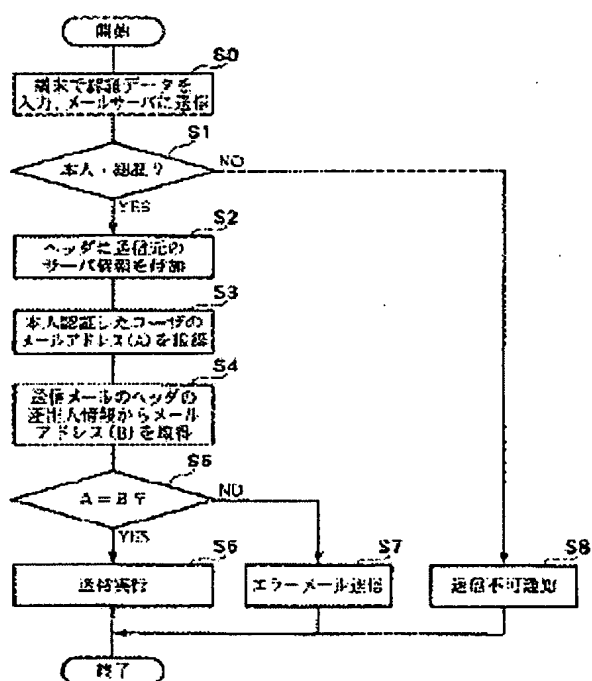
Report a data error here

Abstract of JP2004064215

PROBLEM TO BE SOLVED: To provide an electronic mail system whereby a recipient can discriminate whether a sender is the same as a mail sender in the case of transmitting or receiving electronic mail, and to provide a method for preventing transmission of impersonated electronic mail and a method for preventing the reception of impersonated mail.

SOLUTION: The flowchart of operations in an SMTP server includes: a step S1 wherein the SMTP server (transmission server) authenticates a concerned user at mail transmission; a step S2 of adding server information of a sender to an authentication header when the concerned user is authenticated; a step S3 of acquiring a mail address (A) of the authenticated user; a step S4 of acquiring an mail address (B) from header sender information; a step S5 of comparing the mail address (A) with the mail address (B); and a step S6 of transmitting mail only when they are coincident.

COPYRIGHT: (C)2004,JPO



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-64215

(P2004-64215A)

(43) 公開日 平成16年2月26日(2004.2.26)

(51) Int.Cl.⁷

H04L 12/58

F1

H04L 12/58 I00F

テーマコード(参考)

5K030

審査請求 未請求 請求項の数 8 O L (全 13 頁)

(21) 出願番号 特願2002-216759(P2002-216759)
 (22) 出願日 平成14年7月25日(2002.7.25)

(71) 出願人 000001443
 カシオ計算機株式会社
 東京都渋谷区本町1丁目6番2号
 (74) 代理人 100072383
 弁理士 永田 武三郎
 (72) 発明者 成瀬 健一
 東京都羽村市栄町3丁目2番1号 カシオ
 計算機株式会社羽村技術センター内
 Fターム(参考) 5K030 HA06 KA01 KA06

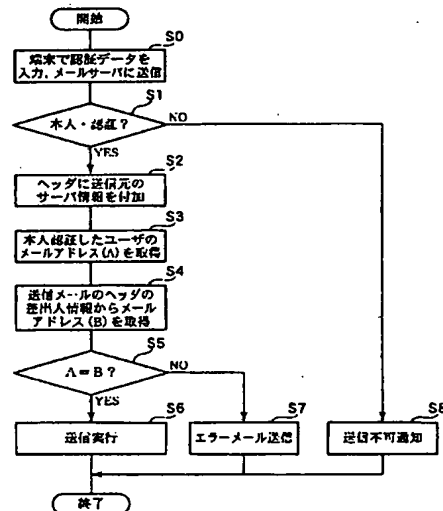
(54) 【発明の名称】 電子メールシステム、電子メールのなりすまし送信防止方法及びなりすまし送信メールの受信防止方法

(57) 【要約】

【課題】 電子メールの送信又は受信の際に受信者がメールの差出人と送信者が同一であるか否かを判断可能な電子メールシステム、電子メールのなりすまし送信防止方法及びなりすまし送信メールの受信防止方法の提供。

【解決手段】 メール送信時にSMTPサーバ(送信サーバ)で本人認証を行い(ステップS1)、本人認証ができた場合は認証ヘッダに送信元のサーバ情報を付加し(ステップS2)、次に、認証したユーザのメールアドレス(A)を取得し(ステップS3)、更に、ヘッダ差出人情報からメールアドレス(B)を取得する(ステップS4)。そして、メールアドレス(A)とメールアドレス(B)を比較し(ステップS5)、一致する場合のみメールを送信する(ステップS6)。

【選択図】 図3



【特許請求の範囲】

【請求項1】

管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する送信サーバと、他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信し、該端末宛てに送信する受信サーバとを備えたメールサーバをインターネットに接続した電子メールシステムであって、
前記メールサーバの送信サーバは、メールの送信時に本人認証を行う認証手段と、送信するメールの差出人情報を取得する差出人情報取得手段と、前記差出人情報取得手段で取得した差出人情報と前記認証手段によって認証された送信メールの送信者情報とを比較する比較手段と、前記比較手段による比較結果が不一致である場合は前記メールの前記送信先端末宛て送信を禁止する送信禁止手段と、を備えたことを特徴とする電子メールシステム

10

【請求項2】

管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する送信サーバと、他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信し、該端末宛てに送信する受信サーバとを備えたメールサーバをインターネットに接続した電子メールシステムであって、
前記メールサーバの送信サーバは、メールの送信時に本人認証を行う認証手段と、送信するメールの差出人情報を読み取る差出人情報取得手段と、前記差出人情報取得手段で取得した差出人情報と前記認証手段によって認証された送信メールの送信者情報とを比較する比較手段と、前記比較手段による比較結果を表す情報を前記メールのヘッダに付加する情報付加手段と、を備えたことを特徴とする電子メールシステム。

20

【請求項3】

管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する送信サーバと、他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信し、該端末宛てに送信する受信サーバとを備えたメールサーバをインターネットに接続した電子メールシステムであって、
前記メールサーバの送信サーバは、メールの送信時に本人認証を行う認証手段と、前記認証手段による本人認証の際に用いたユーザ識別情報を送信するメールのヘッダに付加するユーザ識別情報付加手段と、を備え、
前記メールサーバの受信サーバは、他のメールサーバからインターネットを介して前記メールサーバの管理下の端末宛てメールを受信したとき、該受信メールのヘッダから差出人情報、本人認証の際に用いられたユーザ識別情報、及び送信元サーバ名を取得する提示情報取得手段と、
前記提示情報取得手段によって取得した、前記差出人情報、前記ユーザ識別情報、及び前記送信元サーバ名を該メールサーバの管理下の送信先端末宛てに送信する提示情報送信手段と、前記送信先端末から受信拒否通知を受信したとき、前記受信メールを廃棄する受信メール廃棄手段と、を備えたこと、
を特徴とする電子メールシステム。

30

【請求項4】

前記送信サーバはSMTPサーバであり、前記認証手段による本人認証はメールの送信に先立って入力されたユーザ識別情報及びパスワードと前記メールサーバに登録されているユーザ登録情報との比較により行うことを特徴とする請求項1乃至3記載の電子メールシステム。

40

【請求項5】

前記送信サーバはSMTPサーバであり、前記受信サーバはPOPサーバであって、前記認証手段による本人認証はメールの送信に先立って前記POPサーバで行うPOP認証であることを特徴とする請求項1乃至3記載の電子メールシステム。

【請求項6】

前記差出人情報取得手段は、前記メールサーバが管理下の端末から受信した送信メールの

50

ヘッダ情報に含まれる差出人情報からメールアドレスを取得する手段であることを特徴とする請求項1記載の電子メールシステム。

【請求項7】

管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する際に本人認証を行なう工程と、

本人認証された場合に送信メールのヘッダ情報に含まれる差出人情報を取得する工程と、

前記取得した差出人情報と前記認証された送信メールの送信者情報とを比較する工程と、

前記比較結果が一致しないときは前記送信メールの送信を禁止する工程と、

を備えたことを特徴とする電子メールのなりすまし送信防止方法。

【請求項8】

第1のメールサーバが他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信する工程と、

前記受信メールのヘッダ情報から差出人情報、ユーザ識別情報、及び送信元サーバ名を取得する工程と、

前記取得した、前記差出人情報、ユーザ識別情報、及び送信元サーバ名を第1のメールサーバの管理下の送信先端末宛てに送信する工程と、

前記送信先端末から受信拒否通知を受信したとき、前記受信メールを廃棄する工程と、

を備えたことを特徴とするなりすまし送信メールの受信防止方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子メールの送信者のなりすまし等による不正なメールの送受信を防止する手段を備えた電子メールシステムに関する。

【0002】

【従来の技術】

インターネットの普及によりインターネット経由で電子メールを送受信することができる。電子メールを利用する場合、一般的に、図1に示すように送信時はSMTPサーバ1を、受信時はPOPサーバ3を介してメールの送受信を行っている。

【0003】

また、メールの受信の際に、他人に自分のメールを読まれないように、ユーザID及びパスワードを入力してPOP認証を行って本人認証を行い、メールを読み取るようにしている（つまり、自分の家の郵便受けの鍵を持っている人だけが手紙を読むことができるということと同様である）。

【0004】

一方、メール送信の場合は特に本人認証の必要はない（東京に住んでいる人が大阪から手紙を出すことができるのと同じ）。しかし、だれでも送信できるようにすると第三者が大量のメールを送信し、サーバに過大な負荷をかけるというようなことが可能になるので、最近ではメール送信時にもPOP認証を行うようにしたもの（POP before SMTP）もある。

【0005】

なお、電子メールにおける「なりすまし」に関する先行技術として、▲1▼特開平8-251156号公報開示の技術（なりすましを防止するためにパスワード等の暗号化を行うことを要旨としたもの）、▲2▼特開平9-114719号公報開示の技術（なりすましを防止するために公開鍵方式を導入したもの）、▲3▼特開平11-25050号公報開示の技術（なりすましを防止するためにテンポラリパスワードを発行するようにしたもの）、▲4▼特開2001-266024号公報開示の技術（なりすましによる購入（発注）防止のため、ユーザの携帯電話に購入確認の電子メールを送るようにしたもの）がある。

【0006】

また、電子メールの本人認証における「本人」又は「差出人」に関する先行技術として、

▲5▼特開2000-224221号公報開示の技術（エージェントサーバに関するもの）、▲6▼特開2002-49757号公報開示の技術（インターネットによる融資申し込みに関するもの）、▲7▼特開2002-55982号公報開示の技術（送信済みメールの削除や更新ができるようにしたもの）、▲8▼特開2002-63658（携帯電話を利用したPOS管理システム）がある。

【0007】

【発明が解決しようとする課題】

上記メール送信時の本人認証は第三者のSMTPサーバの利用を制限するものであり、送信するメールの差出人情報の内容のチェックは行われていないため、メール送信者がメールの差出人名、差出人メールアドレスを任意に設定すれば他人になりすましてメールを送信することが出来るという問題点がある。紙の手紙の場合には筆跡などから本人がどうかを判断することもできるが、電子メールの場合にはそのようなこともできない。

10

【0008】

このようなメールの差出人の他者なりすまし対策のために、現在では、差出人に一度メールを送り返し、そのメールを再度送信してもらうことで送信者と差出人が同一であるか否かを判断する場合があるが、差出人にとって同一メールを2度送らなければならないという手間がかかるといった問題点がある。

【0009】

一方、上記先行技術調査の結果である▲1▼～▲3▼の技術はユーザID及びパスワードを盗まれないようにして第三者によるなりすましを防止しようとするものであり、なりすましによる不正な電子メールの送信防止技術とは異なる。また、上記▲4▼の技術は電子メールを確認手段とするものであり、なりすましによる不正な電子メールの送信防止とは無関係である。また、▲5▼～▲8▼の技術は電子メールシステムにおける不正メールの送信防止とは異なる目的でなされたものであり、なりすましによる不正メール防止技術とは異なる。

20

【0010】

本発明は、上記電子メール送信時の本人認証に係わる問題点を解決するためになされたものであり、電子メールの送信又は受信の際に受信者がメールの差出人と送信者が同一であるか否かを判断可能な電子メールシステム、電子メールのなりすまし送信防止方法及びなりすまし送信メールの受信防止方法の提供を目的とする。

30

【0011】

【課題を解決するための手段】

上記課題を解決するために、第1の発明の電子メールシステムは、管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する送信サーバと、他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信し、該端末宛てに送信する受信サーバとを備えたメールサーバをインターネットに接続した電子メールシステムであって、メールサーバの送信サーバは、メールの送信時に本人認証を行う認証手段と、送信するメールの差出人情報を取得する差出人情報取得手段と、差出人情報取得手段で取得した差出人情報と認証手段によって認証された送信メールの送信者情報とを比較する比較手段と、比較手段による比較結果が不一致である場合はメールの送信先端末宛て送信を禁止する送信禁止手段と、を備えたことを特徴とする。

40

【0012】

また、第2の発明の電子メールシステムは、管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する送信サーバと、他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信し、該端末宛てに送信する受信サーバとを備えたメールサーバをインターネットに接続した電子メールシステムであって、メールサーバの送信サーバは、メールの送信時に本人認証を行う認証手段と、送信するメールの差出人情報を読み取る差出人情報取得手段と、差出人情報取得手段で取得した差出人情報と認証手段によって認証された送信メールの送信者情報とを比較する比較手段と、比較手段による比較結果を表す情報をメールのヘッダに付加する情報付加手段と

50

、を備えたことを特徴とする。

【0013】

また、第3の発明の電子メールシステムは、管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する送信サーバと、他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信し、該端末宛てに送信する受信サーバとを備えたメールサーバをインターネットに接続した電子メールシステムであって、メールサーバの送信サーバは、メールの送信時に本人認証を行う認証手段と、認証手段による本人認証の際に用いたユーザ識別情報を送信するメールのヘッダに付加するユーザ識別情報付加手段と、を備え、メールサーバの受信サーバは、他のメールサーバからインターネットを介してメールサーバの管理下の端末宛てにメールを受信したとき、該受信メールのヘッダから差出人情報、本人認証の際に用いられたユーザ識別情報、及び送信元サーバ名を取得する提示情報取得手段と、提示情報取得手段によって取得した、差出人情報、ユーザ識別情報、及び送信元サーバ名を該メールサーバの管理下の送信先端末宛てに送信する提示情報送信手段と、送信先端末から受信拒否通知を受信したとき、受信メールを廃棄する受信メール廃棄手段と、を備えたことを特徴とする。

10

【0014】

また、第4の発明は上記第1乃至第3の発明の電子メールシステムにおいて、送信サーバはSMTPサーバであり、認証手段による本人認証はメールの送信に先立って入力されたユーザ識別情報及びパスワードとメールサーバに登録されているユーザ登録情報との比較により行うことを特徴とする。

20

【0015】

また、第5の発明は上記第1乃至第3の発明の電子メールシステムにおいて、送信サーバはSMTPサーバであり、受信サーバはPOPサーバであって、認証手段による本人認証はメールの送信に先立ってPOPサーバで行うPOP認証であることを特徴とする。

【0016】

また、第6の発明は上記第1の発明の電子メールシステムにおいて、差出人情報取得手段は、メールサーバが管理下の端末から受信した送信メールのヘッダ情報に含まれる差出人情報からメールアドレスを取得する手段であることを特徴とする。

【0017】

また、第7の発明の電子メールのなりすまし送信防止方法は、管理下の端末から受信した送信メールをインターネットを介して送信先端末宛てに送信する際に本人認証を行なう工程と、本人認証された場合に送信メールのヘッダ情報に含まれる差出人情報を取得する工程と、取得した差出人情報と認証された送信メールの送信者情報とを比較する工程と、比較結果が一致しないときは送信メールの送信を禁止する工程と、を備えたことを特徴とする。

30

【0018】

また、第8の発明のなりすまし送信メールの受信防止方法は、第1のメールサーバが他のメールサーバからインターネットを介して管理下の端末宛てに送信されたメールを受信する工程と、受信メールのヘッダ情報から差出人情報、ユーザ識別情報、及び送信元サーバ名を取得する工程と、取得した、差出人情報、ユーザ識別情報、及び送信元サーバ名を第1のメールサーバの管理下の送信先端末宛てに送信する工程と、送信先端末から受信拒否通知を受信したとき、受信メールを廃棄する工程と、を備えたことを特徴とする。

40

【0019】

【発明の実施の形態】

図1は電子メールシステムのハードウェア構成の概略説明図であり、図2は電子メール送受信の概要を示す図である。

図1で、電子メールシステム100は、メールサーバ10と、図示しない複数のメールサーバと接続するインターネット20と、メールサーバ10の管理下の複数の端末(図1では端末30で代表する)からなる。なお、メールサーバ10以外の複数のメールサーバも複数の端末を管理下においている。

50

【0020】

メールサーバ10はSMTPサーバ（送信サーバ）1、メールボックス2、POPサーバ（受信サーバ）3、保存記憶メモリ5（メールボックスと同じメモリでもよい）に管理下の端末ユーザ毎に登録されたメールアドレス、ユーザID及びパスワード等のユーザ情報を登録したユーザ情報テーブル4を備えている。

【0021】

また、SMTPサーバ1及びPOPサーバ3はそれぞれ制御部（図示せず）及びRAM等の一時記憶メモリを備え、SMTPサーバ1は一時記憶メモリにメール送信処理用のプログラムを駐在させてメール送信処理を行い、POPサーバ3は一時記憶メモリにメール受信処理用のプログラムを駐在させてメール受信用処理を行う。また、メールボックス2は大容量の保存記憶メモリからなり、受信メールが呼び出されるまで受信メールを保存する。

10

【0022】

なお、SMTPサーバ1が一時記憶メモリに駐在させるメール送信処理用のプログラム、POPサーバ3が一時記憶メモリに駐在させるメール受信処理用のプログラム、制御プログラム、通信制御プログラムや端末30にインストールされるメールソフト等やHTMLファイルデータは保存記憶メモリ5に確保されているプログラム記憶領域に保存記憶されている。

【0023】

端末30から他の端末宛て送信された電子メール（以下、単にメールと記す）はSMTPサーバ1を介してインターネット20経由で他のメールサーバに送信される。また、他のメールサーバを介して端末30宛て送信されたメールはインターネット20経由でPOPサーバ3が受信してメールボックス2に保管し、端末30に送信する。具体的にはメールを送信する場合は、図2に示すように、大きく4つの区分（段階）に分けることができる。

20

【0024】

まず、第1段階として端末30のユーザが、宛先、タイトル、及びメール本文を入力すると端末30にインストールされているメールソフトによってメールが作成され、ユーザが送信指示をするとメールサーバ10宛てメールが送信される。このとき、メールの差出人情報（差出人名、メールアドレス）がメールのヘッダに「from: 差出人情報」として付加される。

30

【0025】

次に、第2段階として、SMTPサーバ1で上記第1段階で作成したメールを送信先宛てにインターネット20を介して送信する。このとき、メールのヘッダに「Received: from 送信サーバ名」が付加される。

【0026】

そして、第3段階として、送信先の端末を管理するメールサーバ10のPOPサーバ3に他のメールサーバからインターネット20経由でメールが送信される。このとき、メールのヘッダに「Received: from 受信サーバ名」が付加され、メールボックス2に受信したメールが保管（記憶）される。

40

【0027】

最後に、第4段階として端末にインストールされているメールソフト等を利用して上記第3段階で当該端末を管理するメールサーバのメールボックスに保管されているメールをPOPサーバ3を介して読み出す。

【0028】

[第1の実施の形態]

以下、本発明の一実施例について説明する。

本実施の形態では、前述した図2の第2段階でSMTPサーバ1を介してインターネット20経由でメールを送信する場合にSMTPサーバ1を利用するユーザを特定するために本人認証を行うこととする。本人認証を行うことにより第三者がメールを送信しようとしても受け付けられない。本人認証は送信時にユーザID及びパスワードを入力し、SMTP

50

Pサーバ1で認証動作を行う。なお、メール送信の前にメール受信操作を実行してPOP認証を行うようにしてもよい。

【0029】

次に、SMTPサーバ1でメールのヘッダ情報の「from:差出人情報」に記載されている差出人メールアドレスと本人認証したメールアドレスが一致しているかを調べ、一致している場合は従来どおりメールを送信し、一致していない場合は「from:差出人情報」に記載されている差出人メールアドレス又は本人認証したメールアドレスの一方若しくは双方に「差出人が一致していません」といったエラー通知メールを送信する。なお、送信しようとしたメールが自動拡散型のウイルスメールである可能性を考慮し、エラーメールには通常のエラーメールのように本文は添付せず、必要に応じて読めるように構成してもよい。

10

【0030】

図3はメール送信時のSMTPサーバ(送信サーバ)の動作例を示すフローチャートである。

まず、端末30側でメールを送信する際に送信サーバを利用するためにユーザにユーザID及びパスワード等の認証データの入力を促し(ステップ80)、ユーザID及びパスワードが入力されるとSMTPサーバ1に入力されたユーザID及びパスワードが送信され、SMTPサーバ1はメールサーバ1の認証データ保存メモリ(図示せず)に登録されている認証データと受信したユーザID及びパスワードを比較して本人認証を行い、本人認証ができた場合はステップ82に遷移する。また、本人認証ができなかった場合は送信不可とし、メール送信は行わず、ステップ88に遷移する(ステップ81)。

20

【0031】

本人認証ができた場合は、端末30のユーザが入力した、あて先、タイトル、及びメール本文からなるメールが端末30にインストールされているメール送受信プログラムによって作成され、ユーザが送信指示をするとメールサーバ10宛てメールが送信される。このとき、メールの差出人情報(差出人名、メールアドレス)がメールのヘッダに「from:差出人情報」として付加される。端末30から送信メールを受信したSMTPサーバ1は従来と同様にメールのヘッダに送信元サーバ名を含むサーバ情報を付加し(ステップ82)、本人認証したユーザID及びパスワードからユーザのメールアドレス(A)を取得する(ステップ83)。

30

【0032】

次に、SMTPサーバ1は端末30からの送信メールのヘッダ情報である「from:差出人情報」から差出人のメールアドレス(B)を取り出し(ステップ84)、上記ステップ83で取得したメールアドレス(A)とステップ84でヘッダ情報から取り出したメールアドレス(B)が一致しているかを調べ(ステップ85)、メールアドレスが一致している場合は、メール送信者とメールの差出人は一致していると判断して端末30からの送信メールをインターネット20を介して送信先端末宛て送信して端末30から受け取った送信メールに係わる処理を終了する(ステップ86)。

【0033】

また、上記ステップ85でメールアドレスが一致していない場合は、メール送信者とメールの差出人が異なっていると判断して端末30宛てエラーメールを送信して端末30から受け取った送信メールに係わる処理を終了する(ステップ87)。

40

【0034】

また、上記ステップ81で本人認証ができなかった場合は端末30宛て送信不可通知(送信不可メール)を送信して端末30から受け取った送信メールに係わる処理を終了する(ステップ88)。

【0035】

上記図3のフローチャートの構成により、メール送信サーバ(SMTPサーバ)上で、送信メールに付加される差出人情報のメールアドレスと本人認証情報から得られるメール送信者のメールアドレスが異なる場合にはメールを送信しないようにしたので、そのメール

50

サーバの利用者からのメールは本物のメール（つまり、そのメールサーバに登録された端末の真正なユーザが送信したメール）であり、なりすましによる不正なメールではないと判断でき、電子メールシステムに対する信頼性が高まる。また、1回のメールで済ますことができるので、従来のように2度メールを送信して本人確認する手間がかからない。更に、差出人メールアドレスの一部を書き換えて勝手にメール送信を行うウイルスメール等のメールアドレスは本発明により本人認証したユーザのメールアドレスと異なるのでウイルスメールの拡散を防止することもできる。

【0036】

なお、図3のフローチャートのステップ80で本人認証用にユーザID及びパスワード等の認証データを入力し、ステップ81でメール送信サーバ（SMTPサーバ）で本人認証するようにしたが、ステップ80を省略し、ステップ81で、通常、電子メールやインターネットを利用する際にインターネットに接続するため、ブラウザにログインする際の認証データ（つまり、電子メールやインターネットの利用時に入力するユーザIDおよびパスワード）をメール送信サーバに送信して本人認証を行うようにしてもよい。このようにすれば、送信メールの差出人は本人認証が行われていることを意識しなくてもよい。

10

【0037】

また、上記ステップ80でメール受信動作を行い、ステップ81でPOP認証（つまり、メール送信に先だってメール受信操作を行うことにより行われる受信サーバ（POPサーバ）による本人認証）により本人認証を行うようにしてもよい。

【0038】

20

また、上記図3のフローチャートの各ステップは送信サーバで実行可能なプログラムとして構成され、RAM等の一時記憶メモリ（図示せず）に駐在して送信サーバの制御部によりメールの送信時に実行される。

【0039】

（変形例）

図4はメール送信時のSMTPサーバ（送信サーバ）の動作例を示すフローチャートである。

【0040】

上記第1の実施例ではメールの差出人情報が認証された送信者情報（以下、認証者情報と記す）と異なる場合はメールを送信しないように構成したが、メールは差出人名義と被認証者の一致、不一致に係わりなく送信するようにし、差出人名義と被認証者が一致しているか否かを示す情報を新たにヘッダ情報に加えてからメールを送信先端末宛て送信するようにしてもよい。

30

【0041】

具体的には、図4のフローチャートに示すように、図3のステップ85で、差出人情報から得たメールアドレスと本人認証情報から得たメールアドレスが一致する場合は差出人名義と被認証者（つまり、メール送信者）が一致している旨の一致情報をヘッダ情報に付加し（ステップ86-1）、差出人情報から得たメールアドレスと本人認証情報から得たメールアドレスが一致しない場合は差出人名義と被認証者が不一致である旨の不一致情報をヘッダ情報に付加して（ステップ86-2）、メールをインターネット20を介して送信先端末宛て送信する（ステップ86-3）。

40

【0042】

この場合、メールを受信する端末側にインストールされているメール送受信プログラムを、メール受信時に受信メールのヘッダ情報を読み取り、一致、不一致、不明等の情報を差出人名、件名等と一緒に一覧表示できるように構成する。

【0043】

〔第2の実施の形態〕

前記第1の実施例では送信サーバ側で不正メールが否かを判断する処理を行ったが、本実施の形態では受信サーバ側で不正メールが否かを判断する。

【0044】

50

まず、図2に示した第2段階において、SMTPサーバ（送信サーバ）はメール送信の際に本人認証を行い、そのときのユーザIDをメールのヘッダ情報に付加してからメールをインターネット20を介して送信先端末宛て（実際には送信先端末を管理するメールサーバ）に送信する。

【0045】

次に、第3段階として、送信先端末を管理するメールサーバのPOPサーバ（受信サーバ）が上記送信先端末宛てのメールを受信しメールボックスに保存し、受信メールのヘッダ情報から差出人情報（つまり「from: 差出人情報」の内容）、送信元サーバ名（つまり、「Received: from 送信元サーバ名」の内容）、及びユーザIDを取り出す。

10

【0046】

そして、第4段階として、メールの本文を含めた全てのデータをメール受信者が端末にダウンロードする前に、差出人情報、送信元サーバ名及びユーザIDをメール受信者に示し、メール受信者に当該メールのダウンロードの可否を尋ねる。

【0047】

メール受信者は示された情報から、そのメールが正しいメールかを、例えば、差出人メールアドレスと送信元サーバ又はユーザIDが異なっているときは不正メールの可能性がある怪しいメールであるといった判断ができる。ユーザが当該メールを問題のあるメールでないと判断して受信操作を行った場合は送信サーバ側は従来どおりダウンロードに応じ、受信拒否操作を行った場合はメールサーバ側でメールボックスに保存した当該メールを破棄する。

20

【0048】

なお、メールのヘッダ情報中の「Received: from 送信元サーバ名」はメールサーバを経由するたびに付加されるため、1通のメールに複数個付加されている場合があるが、これらは新しいものが順次上（先頭）に付加されるので送信元のサーバを調べるとは一番下（後尾）の「Received: from 送信元サーバ名」の内容を読み取ればよい。

【0049】

図5はメール送信時の送信サーバ（SMTPサーバ）とメール受信時の受信サーバ（POPサーバ）の動作例を示すフローチャートであり、図5(a)はメール送信サーバ側動作例を示し、図5(b)はメール受信サーバの動作例を示す。

30

【0050】

まず、図5(a)に示すように、端末30側でメールを送信する際に送信サーバを利用するためにユーザにユーザID及びパスワード等の認証データの入力を促し（ステップT0）、ユーザID及びパスワードが入力されるとSMTPサーバ1に入力されたユーザID及びパスワードが送信され、SMTPサーバ1はメールサーバ1の認証データ保存メモリ（図示せず）に登録されている認証データと受信したユーザID及びパスワードを比較して本人認証を行い、本人認証ができた場合はステップT2に移移する。また、本人認証ができなかった場合は送信不可とし、メール送信は行わず、ステップT5に移移する（ステップT1）。

40

【0051】

本人認証ができた場合は、端末30のユーザが入力した、あて先、タイトル、及びメール本文からなるメールが端末30にインストールされているメール送受信プログラムによって作成され、ユーザが送信指示をするとメールサーバ10宛てメールが送信される。このとき、メールの差出人情報（差出人名、メールアドレス）がメールのヘッダに「from: 差出人情報」として付加される。端末30から送信メールを受信したSMTPサーバ1はメールのヘッダにユーザIDを付加する（ステップT2）。

【0052】

更に、従来と同様にメールのヘッダに送信元サーバ名を含むサーバ情報を付加し（ステップT3）、端末30からの送信メールをインターネット20を介して送信先端末宛て送信

50

して端末30から受け取った送信メールに係わるSMTPサーバ側の処理を終了する(ステップT4)。

【0053】

また、上記ステップT1で本人認証ができなかった場合は端末30宛て送信不可通知(送信不可メール)を送信して端末30から受け取った送信メールに係わる処理を終了する(ステップT5)。

【0054】

次に、図5(b)に示すように、端末30からの送信メールの宛先端末を管理するメールサーバ側ではPOPサーバ(受信サーバ)が当該メールを受信してメールボックスに保存する。また、この際、POPサーバは受信メールのヘッダにサーバ情報を付加する(ステップT11)。

10

【0055】

次に、POPサーバは受信メールのヘッダからそのメールの差出人情報を取り出し(ステップT12)、次に受信メールのヘッダから、メール送信者のユーザIDを取り出す(ステップT13)。更に、受信メールのヘッダから送信サーバ名を取り出す(ステップT14)。

【0056】

次に、POPサーバは受信端末に上記ステップT12~T14でヘッダから取り出したメールの差出人情報、メール送信者のユーザID及び送信サーバ名を受信端末宛て送信し、ユーザに提示する(受信端末側ではこれら情報を受信するとメール送受信プログラムがこれらの情報を一覧表示してユーザにメール受信の可否の指示(操作)を促す)(ステップT15)。

20

【0057】

メール受信者は端末に一覧表示されたメールの差出人情報、メール送信者のユーザID及び送信サーバ名を見てこのメールをダウンロードするか否かを判断し、判断結果に基づいて指示(ダウンロード許可又は不許可指示)を行い、端末はユーザの指示(ダウンロード許可通知又は不許可通知)をPOPサーバ宛て送信するので、POPサーバは受信した通知の内容を調べ、許可通知の場合にはステップT17に遷移し、不許可通知の場合にはステップT18に遷移する(ステップT16)。

【0058】

許可の場合には従来とおりメールのダウンロード処理を行なって当該受信メールに係わるPOPサーバ側の処理を終了する(ステップT17)。また、不許可の場合には当該メールを廃棄して(具体的にはメールボックスから削除して)当該受信メールに係わるPOPサーバ側の処理を終了する(ステップT18)。

30

【0059】

上記図5のフローチャートに示した構成により、端末側でメールを受信する前にメール送信者の情報を知ることができるため、メール本文の受信を行う前にユーザが差出人名義とメール送信者が一致しているかを判断できるので、不正メールの可能性のある怪しいメールを受信しないといった選択が可能となる。また、送信者が特定できるので、ウイルスメールの送信元を調べることが容易にできる。

40

【0060】

なお、図5(a)のフローチャートのステップT0で本人認証用にユーザID及びパスワード等の認証データを入力し、ステップT1でメール送信サーバ(SMTPサーバ1)で本人認証するようにしたが、ステップT0でメール受信動作を行い、ステップS1でPOP認証(つまり、メール送信に先だってメール受信操作を行うことにより行われる受信サーバ(POPサーバ3)による本人認証)により本人認証を行うようにしてもよい。

【0061】

また、図5(b)のフローチャートのステップT15で差出人情報、ユーザID及び送信サーバ名の3つを予めユーザに提示するようにしたが、送信日時、件名等の情報も取得するようにして同時に提示してもよい。

50

【0062】

なお、上記図5(a)のフローチャートの各ステップは送信サーバで実行可能なプログラムとして構成され、RAM等の一時記憶メモリ（図示せず）に駐在して送信サーバの制御部によりメールの送信時に実行される。また、上記図5(b)のフローチャートの各ステップは受信サーバで実行可能なプログラムとして構成され、RAM等の一時記憶メモリ（図示せず）に駐在して受信サーバの制御部によりメールの受信時に実行される。

【0063】

（変形例）

上記第2の実施例では、メール送信時に送信者のユーザIDを付加するようにしたが（図5(a)のステップT2）、本発明の電子メールシステム以外の電子メールシステムを採用しているメールサーバから送信されるメールのように、ユーザIDが付加されていないメールを受信した場合も本発明の電子メールシステムを利用できるようにすることができる。この場合、メール受信する側では一部の情報（ユーザID）が欠落するが、図5(b)のステップT13でヘッダからユーザIDを取り出す際に、ヘッダ内容を調べ、ユーザIDがない場合はスペースを取り出したものとして扱うことにより、ユーザは差出人情報及び送信サーバ名からダウンロードするかどうかを判断できる。

10

【0064】

以上、本発明のいくつかの実施例について説明したが本発明は上述した各実施例に限定されるものではなく、種々の変形実施が可能であることはいうまでもない。

また、本発明の適用範囲は図1に示したような構成のメールサーバに限定されず、例えば、サーバを運営するフロパイダ、メールソフト又はプログラム、メールソフト又はプログラムを動作させるパソコン、メールソフト又はプログラムを記憶する記憶媒体、メールソフト又はプログラムを記憶するネットワーク（インターネットに限定されない）上のサーバ、ネットワーク上を伝送するメールソフト又はプログラムにも適用されるものである。

20

【0065】

【発明の効果】

上記説明したように、第1の発明の電子メールシステムによれば、メール送信サーバ上で、送信メールに付加される差出人名義と本人認証されたメール送信者情報から得られるメール送信者が異なる場合にはそのメールの送信を禁止するので、そのメールサーバの利用者から送信されるメールはなりすましによる不正なメールではないメールとなり、電子メールシステムに対する信頼性が高まる。

30

【0066】

また、1回のメールで済ますことができるので、従来のように2度メールを送信して本人確認する手間がかからない。更に、差出人情報（例えば、メールアドレスの一部）を書き換えて勝手にメール送信を行うウイルスメールについても送信を禁止できるので、ウイルスメールの拡散を防止することもできる。

【0067】

また、第2の発明の電子メールシステムによれば、メール送信サーバ上で、送信メールに付加される差出人名義と本人認証されたメール送信者情報から得られるメール送信者の異同に応じた情報をメールのヘッダに付加するため、メールの宛先端末ではユーザは受信したメールのヘッダを読んで、メール本文を受信するかどうかを判断できるので、なりすましによる不正なメールの受信を防止することができる。また、第1の発明と同様に、1回のメールで済ますことができるので、2度メールを送信して本人確認する手間がかからない。更に、差出人情報を書き換えて勝手にメール送信を行うウイルスメールについても受信を防止できるので、ウイルスメールの拡散を防止することもできる。

40

【0068】

また、第3の発明の電子メールシステムによれば、端末側でメールを受信する前にメール送信者の情報を知ることができるため、メール本文の受信を行う前にユーザが差出人名義とメール送信者が一致しているかどうかを判断できるので、不正メールの可能性のある怪しいメールを受信しないといった選択が可能となる。また、送信者が特定できるので、ウイ

50

ルメールの送信元を調べることが容易にできる。

【0069】

また、第4の発明の電子メールシステムでは、本人認証をPOP認証で行うことができるため、送信サーバ側に認証手段としてのプログラムを必要とせず、その分メールサーバのプログラム構成が簡単になる。

【図面の簡単な説明】

【図1】電子メールシステムのハードウェア構成の概略説明図である。

【図2】電子メール送受信の概要を示す図である。

【図3】メール送信時のSMTPサーバ（送信サーバ）の動作例を示すフローチャートである。

10

【図4】メール送信時のSMTPサーバ（送信サーバ）の動作例を示すフローチャートである。

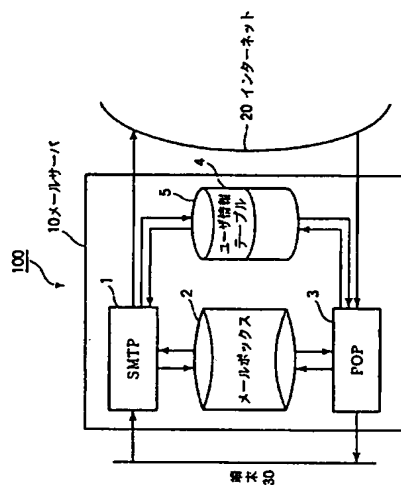
【図5】メール送信時の送信サーバ（SMTPサーバ）とメール受信時の受信サーバ（POPサーバ）の動作例を示すフローチャートである。

【符号の説明】

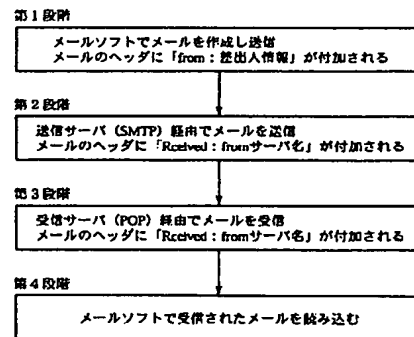
- 1 SMTPサーバ（送信サーバ）
- 2 メールボックス
- 3 POPサーバ（受信サーバ）
- 4 ユーザ情報テーブル（ユーザ登録情報）
- 10 メールサーバ
- 20 インターネット
- 30 端末

20

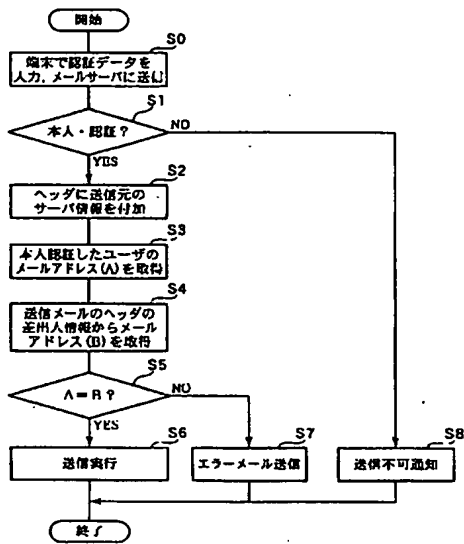
【図1】



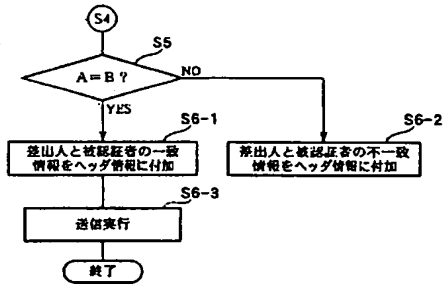
【図2】



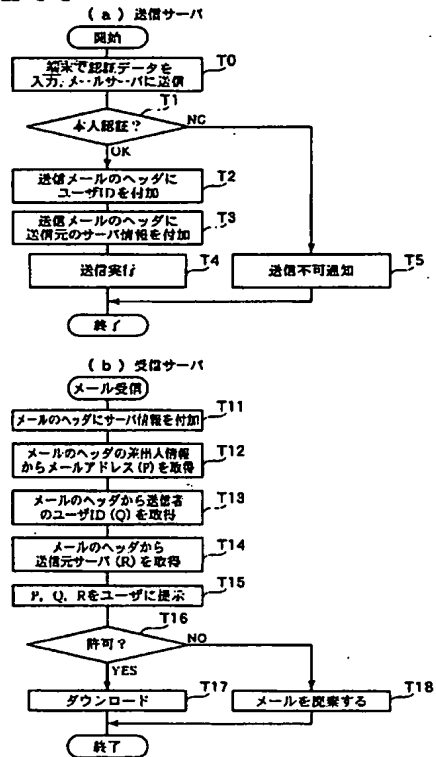
【図3】



【図4】



【図5】



© EPODOC / EPO

N - JP2004064215 A 20040226
 IPD - 2002-07-25
 A - CASIO COMPUTER CO LTD
 I - NARUSE KENICHI
 T - ELECTRONIC MAIL SYSTEM, METHOD FOR PREVENTING TRANSMISSION OF IMPERSONATED ELECTRONIC MAIL, AND METHOD FOR PREVENTING RECEPTION OF IMPERSONATED MAIL
 AB - PROBLEM TO BE SOLVED: To provide an electronic mail system whereby a recipient can discriminate whether a sender is the same as a mail sender in the case of transmitting or receiving electronic mail, and to provide a method for preventing transmission of impersonated electronic mail and a method for preventing the reception of impersonated mail.
 - SOLUTION: The flowchart of operations in an SMTP server includes: a step S 1 wherein the SMTP server (transmission server) authenticates a concerned user at mail transmission; a step S 2 of adding server information of a sender to an authentication header when the concerned user is authenticated; a step S 3 of acquiring a mail address (A) of the authenticated user; a step S 4 of acquiring an mail address (B) from header sender information; a step S 5 of comparing the mail address (A) with the mail address (B); and a step S6 of transmitting mail only when they are coincident.
 - COPYRIGHT: (C) 2004,JPO
 I - H04L12/58&100F
 T - 5K030/HA06; 5K030/KA01; 5K030/KA06
 C - H04L12/58
 CAI - H04L12/58
 CCI - H04L12/58
 IP - JP20020216759 20020725
 IR - JP20020216759 20020725
 AMN - 31938425
 PD - 2004-02-26

© WPI / Thomson

IN - 2004-244088 [23]
 IPD - 2002-07-25
 PD - 2004-02-26
 IP - JP20020216759 20020725
 A - (CASK) CASIO COMPUTER CO LTD
 PY - CASK
 N - NARUSE K
 T - E-mail system using Internet, compares authenticated e-mail address and e-mail address which is acquired from header sender information, for mail transmission
 AB - NOVELTY :
 A simple mail transfer protocol (SMTP) server performs proper identification (ID) authentication during mail transmission. The server information is added to the authenticated header, when the ID is authenticated. The authenticated e-mail address is compared with the e-mail address which is acquired from header sender information. The e-mail is transmitted only if addresses matches during comparison.
 - DETAILED DESCRIPTION :
 INDEPENDENT CLAIMS are also included for the following: (1) impersonation transmitting prevention method; and (2) reception prevention method.
 - USE :
 For transmitting e-mail using Internet.
 - ADVANTAGE :
 Prevents spreading of virus mail, and reception of the irregular mail by impersonation. Enables investigating sending station of a virus mail, easily.
 - DESCRIPTION OF DRAWINGS :

The figure shows the flowchart explaining the operation of the SMTP server. (Drawing includes non-English language text).

PN - JP2004064215 A 20040226 DW200423
NC - 1
IW - MAIL SYSTEM COMPARE AUTHENTICITY ADDRESS ACQUIRE HEADER SEND INFORMATION
TRANSMISSION
IC - H04L12/58
MC - T01-N01C T01-N02B1 W01-A05B
DC - T01 W01